Create a detailed***Executive Report*** about your project and submit it for evaluation.  This report usually totals approximately 20 to 30 pages, double-spaced (**but there is no minimum** or maximum page count).

A.  Describe the consensus-based policies developed for the solution to your cybersecurity problem, including standards and practices that were adopted to facilitate implementation of the solution and a description of the cybersecurity problem being addressed.

1.  Summarize how the solution supports decision-making capabilities and the needs of the environment where the solution was implemented.

B.  Describe how your solution meets the following cybersecurity assurance criteria:

•   promotes automation in cybersecurity

•   improves and modernizes security

•   implements industry-standard security tools and infrastructure or environment

C.  Explain how your solution addresses the following data collection and implementation elements:

•   collects digital evidence, including data for analysis or forensics

•   implements confidentiality, integrity, and availability

D.  Explain how your solution investigates and mitigates cybersecurity incidents and crimes within the environment where the solution was implemented.

E.  Describe the cybersecurity plans, standards, or procedures that were developed for the solution.

1.  Explain how the solution is aligned with cybersecurity initiatives or regulatory compliance in the environment where the solution was implemented.

2.  Summarize the applications, source code, executable files, tools, installation guides, or user guides developed in conjunction with the solution.

F.  Discuss the post-implementation environment, including new systems implemented, new processes developed, or network diagrams created demonstrating the new infrastructure.

1.  Describe the efficiency of the solution.

2.  Analyze the new data (e.g., new reports, logs, processes in place) collected, including how the solution will impact business processes.

3.  Describe the summative evaluation plan, including a plan of action and milestones.

a.  Describe any control deficiency analysis resulting from your testing plan. Or if a controlled deficiency analysis was not required, explain why.

4.  Discuss post-implementation risks, including their likelihood, organizational impact, and mitigation.

5.  Explain how the security solution meets each of the project stakeholder needs, including a description of the stakeholder needs.

a.  Analyze how the changes resulting from the new solution affect stakeholders.

G.  Describe the post-implementation maintenance plan for the solution.

H.  Describe the cybersecurity domain from the attached “List of Cybersecurity Domains” that your solution addresses.

I.  Provide **one**original artifact (e.g., security policy, procedure, **network diagram**) of the completed project.

J.  Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.

K.  Demonstrate professional communication in the content and presentation of your submission.